European Review of Digital Administration & Law - Erdal
2021, Volume 2, Issue 2, pp. 45-52
ISSN 2724-5969 - ISBN 979-12-5994-752-9 - DOI 9791259947529 06

Regulating Distributed Ledgers as Legal Institutions Based in Trust Services

Ignacio Alamillo-Domingo
(Researcher - iDerTec - University of Murcia)

ABSTRACT On 3 June 2013, Margrethe Vestager, Executive Vice-President of the European Commission for a Europe fit for the Digital Age, and Thierry Breton, Commissioner for the Internal Market, presented in Brussels the expected text of the proposal to amend Regulation (EU) No 910/2014 of 23 July 2013 ('eIDAS Regulation') to establish a framework for the European Digital Identity (COM (2021) 281 final, or "eIDAS 2 Proposal"), which fosters and gives full legal validity to the electronic ledgers. Distributed ledger technologies such as blockchains offer highly relevant opportunities for the transformation of digital processes by sustaining data and document processing that until the emergence of these technologies required third-party databases. In this article we present the fundamental features of these technologies, and we introduce the new regulation proposed in relation to them into European Union law.

1. *A brief introduction to (distributed) electronic ledgers*

Distributed ledger technologies (DLTs) and blockchain technology allow for the creation of an unalterable and completely decentralised type of ledger (distributed ledger), which enables new applications, with a very important transformative potential in all domains[1].

An electronic ledger is an information store that maintains final and final transaction records. While the general concept of ledger was originally defined in accounting and financial practice, it can be used for the recording of any type of transaction, such as movements and transfers of movable property.

A highly desirable property of a ledger is resistance to manipulation; in other words, the transaction records, once entered in the general ledger, are extremely difficult to alter by design and cannot be modified without the alteration being evident, whether deliberate or accidental, malicious, or benign. Although it is usually assumed that the information contained in the blockchain is unalterable, there are mechanisms that allow for its controlled modification, using techniques such as the use of chameleonic hashes[2], for example to use when it is legally necessary to delete information[3], so we should refer to relative immutability.

A distributed ledger has its entries stored in a series of nodes in a network, rather than in a single location. In this way, the different nodes of the network can be owned by various entities that interact with each other, having a copy of the ledger.

Distributed ledger (DLT) technologies allow the operation and use of distributed ledgers. A distributed ledger can be defined as a ledger shared between a set of DLT nodes and synchronised between DLT nodes through a consensus mechanism[4].

From an abstract point of view, distributed ledger technology allows the updating of all nodes in a network, in a distributed computing environment, of the current state of the world, thus allowing a shared state of trust to be conferred on a distributed system; in other words, when an action is recorded using these

* Article submitted to double-blind peer review.

[1] B. Cappiello and G. Carullo, G., *Introduction: The Challenges and Opportunities of Blockchain Technologies*, in *Blockchain, Law and Governance*, B. Cappiello and G. Carullo (eds.), Cham, Springer Nature Switzerland AG, 2021, 1; G. Carullo, *The Role of Blockchain in the Public Sector: An Overview* in B. Cappiello and G. Carullo (ed.), *Blockchain, Law and Governance*, 55; D. Hellwig, G. Karlic and A. Huchzermeier, *Build Your Own Blockchain*, Cham, Springer Nature Switzerland AG, 2020, 173 M. Swan, *Blockchain. Blueprint for a new economy*, Sebastopol, O'Reilly Media Inc, 2020, 27; A.N. Turi, *Blockchain and Distributed Ledger Technology Applications*, in A.N. Turi (ed.), *Technologies for Modern Digital Entrepreneurship: Understanding Emerging Tech at the Cutting-Edge of the Web 3.0 Economy*, Berkeley (CA), Apress, 2020, 123, doi.org/10.1007/978-1-4842-6005-0_4.

[2] G. Ateniese, B. Magri, D. Venturi and E. Andrade, *Redactable Blockchain – or – Rewriting History in Bitcoin and Friends*, in Vv.Aa., *IEEE European Symposium on Security and Privacy* (EuroS&P), Washington and Tokyo, CPS, 2017, 111, doi.org/10.1109/EuroSP.2017.37.

[3] C. Zhang, Z. Ni, Y. Xu, E. Luo, L. Chen and Y. Zhang, *A trustworthy industrial data management scheme based on redactable blockchain*, in *Journal of Parallel and Distributed Computing*, vol. 152, 2021, 167.

[4] ISO 22739:2020. Blockchain and distributed ledger technologies – Vocabulary.

technologies, what really happens is that that register is carried out in a large number of different places, rather than a single centralised place, so we can consider such a register to be authentic.

DLT systems are designed to implement distributed ledgers, a major challenge due to the need to agree and maintain transaction logs in the distributed ledger[5]. In a DLT system, consensus ensures that each replicated version of a transaction is the same on all nodes where it is stored, and that its content is generally agreed between the parties involved in the transaction. In addition, the set of records in the distributed ledger should be verifiable and auditable, one of the main objectives of DLT to provide non-disputable online transaction records between the parties.

As regards the DLT node we have already referred to, it is defined as a device or process that participates in a network and stores a complete or partial replica of the ledger records, and a general ledger record is defined as a registry containing transaction records, summary values of transactions, records or references to transaction records recorded in a distributed ledger[6].

Again, blockchain systems are a subset of distributed ledger technologies in which the status of a distributed ledger is maintained by processing lots of transactions in secure cryptographically known as blocks data structures[7]. To exemplify this explanation, Figure 1 shows the structure of an Ethereum block[8].

A valid protocol must ensure that each block is cryptographically linked to an immediately preceding block that forms a single sequence of blocks over time. The complete sequence of cryptographically associated blocks forms a globally accessible append-only data structure, the blockchain, which provides the canonical version of the global transaction history.

To ensure that the ledger update process results in a single ledger status for a given block, blockchain protocols include a consensus mechanism that provides a total order of all intra-block transactions. The collective action of all nodes in the blockchain system works as a time stamp server that validates pending transactions and updates the current state of the ledger by adding blocks sequentially to the blockchain.

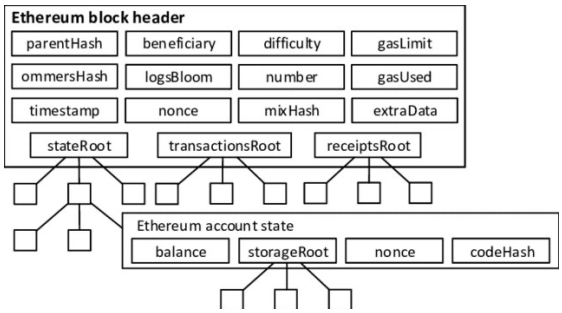

Figure 1. Structure of an Ethereum block

To implement a distributed ledger, blockchain systems therefore require (1) a mechanism to distribute new blocks to all nodes, (2) a mechanism to validate transactions, and (3) a mechanism to ensure consistency of all copies of the blockchain. There is a rich variety of consensus mechanisms, including Proof of Work, employed in open networks, such as Bitcoin and Ethereum, or Proof of Authority, employed in permissioned networks, public or private, such as Alastria or the European Blockchain Services Infrastructure (EBSI).

We are therefore referring to a system in which we can write any information we want, forwarding a transaction, either acting as a network node or through a network node; from that moment on, that transaction, and the information it contains, will be copied to all other nodes on the network, so none of them will be able to delete that information unilaterally. Only with the participation of a significant number of nodes –depending on the consensus protocol– could an insertion into the network in question be eliminated, so there is no need to rely on any of them, and that an insertion of information, or the result of the execution of a transaction, which has spread within the network, be considered to be "true".

This does not mean, of course, that the information itself is "true", but that it is true that that information was recorded, and not another different information, or that that a movement was made between accounts, and not a different one. Similarly, when a qualified electronic signature is used to authenticate a private document, the content of the document is attributable to the signatory, regardless of whether the content is true or not. For example,

[5] ISO 23257. Blockchain and distributed ledger technologies — Reference architecture.
[6] ISO 22739:2020.
[7] ISO 23257.
[8] I. Weber, Q. Lu, A.B. Tran, A. Deshmukh, M. Gorski, and M. Strazds, *A Platform Architecture for Multi-Tenant Blockchain-Based Systems*, presented at IEEE International Conference on Software Architecture (ICSA), 2019, doi.org/10.1109/ICSA.2019.00019, 2019.

when a false declaration is made and signed, the document is authentic because it is imputable to the signatory, but its content is false. The same is true, in essence, of distributed registration technologies.

What really differentiates both cases have to do with one of the most unique particularities of the electronic document and consists of the possibility of making infinite identical copies of it, all of them with the condition of original, simultaneously.

In fact, let's imagine that we write a contract in a PDF file, and we sign it electronically. On paper the physical copy containing the signature would be original, and given the impossibility of duplicating it, we will need at least two copies, each signed by both parties, to formalise the contract (which, for this reason, is signed 'in duplicate copy'), each of them having this condition exclusively. On the contrary, on the said electronic medium and PDF format, it is only necessary to sign one copy. it can be reproduced endlessly, by simply copying the corresponding computer file, such as when stored on a hard or removable disk, when it is sent by email or uploaded to a file storage service in the Cloud (for which, in addition, the ritual reference to 'duplicate copy' should be abandoned today favour of an 'electronic single copy').

The example just given shows one of the advantages of electronically signing a document, but it also gives a good account of one of its limitations, which can be quickly sensed. It is not a useful mechanism for those cases where the transfer of a value occurs through the delivery of a document.

DLT/Blockchain allows, for the first time in history, applications such as the execution of endorsements, thus facilitating the implementation of electronic securities of all kinds, or the efficient and unalterable implementation of unalterable legal and administrative registers, in particular those that collect transfers of assets or allocations of privileges, which are carried out by means of the corresponding electronic signature of the natural person or electronic seal of the legal person of the transaction referred to the DLT/Blockchain system.

In this respect, an analysis of the properties of the electronic seal provided for in Regulation (EU) No 910/2014 of 23 July 2014 ('eIDAS Regulation'), with and without the use of blockchain technologies, has already been carried out[9], concluding in its equivalence, so that the choice of one or the other technique depends only on the case of use. Since this is true from a technical point of view, the fact remains that the eIDAS Regulation limits the cross-border recognition of signature/sealing systems to certain technical formats, which currently do not support DLT/Blockchain. Therefore, various proposals have been made to allow signatures/seals on DLT/Blockchain based on qualified certificates using current technologies, based on the ITU-T standard Rec. X.509[10].

Until the emergence of these technologies, the approach to the computerisation (today we would probably talk about digitisation) of securities of all kinds consisted of replacing the use of the corresponding title with its "notification into account"; that is to say, by the entry in a centralised register of titles and subsequent amendments thereto. This has happened in secondary markets, in cash transfers and other payment transactions, or in transportation tickets.

However, with distributed ledger technologies, we now can electronically transfer titles through electronic endorsement, eliminating the need for such centralised registers. In this area it is inescapable to refer to the possibility of implementing, through distributed registration technologies, traceability systems for all types of objects, both in the electronic world and in the physical world, using the technique of "tokenisation", especially when tokens represent assets.

But it is not only in this domain in which applications of distributed registry technologies have been proposed, since this technology would allow the implementation of guarantees of authenticity in the currently centralised databases, preventing the undetectable modification of the records contained therein, something important both in the private sector and in the public sector, given the legal requirements regarding the integrity of databases, especially in accounting and tax regulations.

From a public sector perspective, DLT seems

[9] V. Alimehaj, A. Halili, R. Dervishi, V. Neziriand and B. Rexha, *Analysing and comparing the digital seal according to eIDAS regulation with and without blockchain technology*, in *International Journal of Information and Computer Security*, vol. 14, n. 2, 2021, 171.

[10] M. Turkanović and B. Podgorelec, *Signing Blockchain Transactions Using Qualified Certificates*, in *IEEE Internet Computing*, vol. 24, n. 6, 2020, 39.

particularly appropriate as a supporting technology for decentralised digital identity management and records management, presenting a significant potential for the transformation of secure document management in the public sector, especially as regards digital signatures, certificates, and document authentication[11], which applies also to other sectors as well. However, it should not be forgotten that this technology has inherent limitations, both technological and socio-economic, especially depending on the consensus mechanism used and the governance model of the network, which must be considered before adopting its widespread use[12].

2. *The general notion of trust service in the eIDAS Regulation*

According to Article 3(16) of the eIDAS Regulation, a trust service "means an electronic service normally provided for remuneration which consists of: (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or (b) the creation, verification and validation of certificates for website authentication; or (c) the preservation of electronic signatures, seals or certificates related to those services".

This Article does not properly contain a definition or concept of trust service, but rather an enumeration of information society services (or digital services, using a more modern terminology used by the European Union institution) which, precisely because they are included in this closed list, are considered to be "trustworthy".

The designation of "trust service" contained in the eIDAS Regulation constitutes an evolution and, at the same time, a semantic extension on the name of the "certification service" used in the eSign Directive. It is an expression derived from the fact that these services enable confidence in the business processes in which they are used, possibly thanks to the legal effects associated with said services. This notion of "trust service", also referred to as "reliable service" or "trusted service", is not an invention of the eIDAS Regulation, but rather has been used for a long time by market operators, as well as by scholars[13].

Thus, according to Recital (2) of the eIDAS Regulation, it "seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union", for which it is necessary to go beyond the regulation of electronic signature, which did not offer "a comprehensive cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions".

The eIDAS Regulation, therefore, pursued the creation of a uniform law for the internal market, providing harmonised legal norms in relation to various services, which in fact already operated on similar technical standards, and offered the possibility of coordinating the different basis of laws for electronic government and digital society globally, although it also posed important challenges[14].

Trust services can be described as those technologies that can be trusted, modifying the user's perception regarding the vulnerability of a process to which they are incorporated. For this, the user must be able to recognise a trust service, in fact, as secure and reliable enough. To do this, the approach of the eIDAS Regulation is the creation of a reinforced level of services of trust,

[11] S. Ølnes and A. Jansen, *Blockchain Technology as a Information Infrastructure in the Public Sector*, in C.G. Reddick, M.P. Rodriguez and H.J. Scholl (eds.), *Blockchain and the Public Sector. Theories, Reforms and Case Studies*, Cham, Springer Nature Switzerland AG, 2021, 19.

[12] A. Buldas, D. Draheim, T. Nagumo and A. Vedeshin, *Blockchain Technology: Intrinsic Technological and Socio-Economic Barriers*, in T. K. Dang, J. Küng, M. Takizawa, & T. M. Chung (eds.), *Future Data and Security Engineering*, Cham, Springer Nature Switzerland AG, 2020, 17; Gamage, H.T.M., Weerasinghe, H.D. and N.G.J. Dias, *A Survey on Blockchain Technology Concepts, Applications, and Issues*, *SN Computer Science*, vol. 1, n. 114, 2020, 12.

[13] J. Dumortier and N. Vandezande, *Critical Observations on the Proposed Regulation for Electronic Identification and Trust Services for Electronic Transactions in the Internal Market*, ICRI Research Paper 9, 2012; J. Dumortier and N. Vandezande, *Trust in the proposed EU regulation on trust services?*, in *Computer Law & Security Review*, vol. 28, n. 5, 2012, 573; A. Jøsang, R. Ismail and C. Boyd, *A survey of trust and reputation systems for online service provision*, in *Decision Support Systems*, vol. 43, n. 2, 2007, 619; J. Ølnes, *A Taxonomy for Trusted Services*, in B. Schmid, K. Stanoevska Slabeva, & V. Tschammer (eds.), *Towards the E-Society: E-Commerce, E-Business, and E-Government,* Boston, MA, Kluwer Academic Publishers, 2002, 37.

[14] G. Borges, *The Draft Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, COM (2012) 238*, Presentation at the Workshop on Electronic Identification and Trust Services, Brussels, 2012.

which is significant in the sense that the trust in these services seems to be born from the fact that they are legally regulated, rather than only in their own technical characteristics[15].

Article 3(17) of eIDAS Regulation provides the notion of a "qualified trust service", defining it as "a trust service that meets the applicable requirements laid down in this Regulation", which differentiates two "reliance levels":

- The non-qualified trust service level, which is not practically regulated and has not an associated legal effect in the eIDAS Regulation, to the trust service or to the institution supported by the trust service; in this case, the user must build his own internal state of trust with respect to the service. For example, a person can consider a password provided by her financial institution as being secure enough for signing a contract.
- The qualified trust service level, which is highly regulated, and receives a particular recognition of legal effects, something which should be an incentive to its adoption, a promise that has not always been fulfilled due to several inhibitors[16]. In this case, this explicit legal recognition is the one that allows the user to recognise the service as reliable, so we can assume that these services will be developed earlier and in greater volume than those that do not enjoy this condition.

It should also be noted that the eIDAS Regulation contains a closed list of trusted services in order to delimit the scope of the uniform European regulation but that Member States may define other trust services as well as maintain (or introduce) national provisions, in accordance with Union law, concerning trust services of confidence, provided that such services are not fully harmonised by this Regulation, considerations which show the central objective of the regulation, which is none other than to guarantee the free movement of these services in the internal market, by means of a minimum set of harmonised standards.

One consequence of this model is the more than possible divergence in the catalogue of trust services in the different jurisdictions of the European Union, as the business sector is constantly generating new services, based on technological innovation. For instance, Belgium has regulated a national trust service consisting in a secure document archive, with a specific legal effect, both as non-qualified and qualified service.

Under the eIDAS Regulation, all trust service providers are subject to some obligations (e.g., Article 19, with regards to appropriate technical and organisational measures to manage the risks posed to the security of the trust services) and qualified trust service providers must comply with a set of strict legal obligations commonly applicable to all services (Article 24) and specific requirements for each qualified trust service).

In contrast to the previous legislation, where the provision of certification services was not subject to any kind of previous licence, the eIDAS Regulation opts for a regulatory orientation of prior administrative authorisation in relation to the provision of qualified trust services[17], while maintaining the *ex-post* supervision model for non-qualified services.

Indeed, Article 21 (1) of the eIDAS Regulation sets out that a provider, who does not have a qualification, to begin its activity relating to qualified services, must submit to the supervisory body a notification of his intention together with a conformity assessment report issued by a conformity assessment body, whereas Article 17 (3) (a) (4) (g) stipulates that the national body will carry out prior supervision and the award of the qualification, and that the service cannot be started until such qualification has been obtained (Article 21 (3)), and it has been publicly disseminated through the mechanism provided for in Article 22 of the eIDAS Regulation (the Trusted List). Although with a somewhat obscure terminology, this is an administrative authorisation, which must be granted under the relevant administrative procedure, within the national legislation framework.

In addition, the qualified provider of trusted

[15] I. Alamillo-Domingo, *SSI eIDAS Legal Report. How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market*, 2020, https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf.

[16] H. Roβnagel, *On diffusion and confusion - Why electronic signatures have failed,* in S. Fischer-Hübner, S. Furnell and C. Lambrinoudakis (eds.), *Trust and Privacy in Digital Business. 3rd International Conference on Trust and Privacy in Digital Business, TrustBus 2006*, Vol. LNCS 4083, Springer, 2006; A. Srivastava, *Resistance to change: Six reasons why businesses don't use e-signatures*, in *Electronic Commerce Research*, vol. 11, n. 4, 2011, 366.

[17] D. Gobert, *Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS): analyse approfondie*, in www.droit-technologie.org, 2015; M. Rico-Carrillo, *El Reglamento europeo sobre identificación y servicios de confianza electrónicos*, in *Revista General de Derecho Europeo,* vol. 35, 2015.

services must pass a conformity assessment at least every two years and send it to the supervisor, as determined by Article 20 (1) of the Regulation, as well as accept any audit performed by the supervisor, or additional assessments of conformity that it imposes on it, pursuant to the provisions of paragraph 2 of Article 20 of the eIDAS Regulation.

As seen in Figure 2, technical standards play a significant role[18], sometimes being applicable in a voluntary basis (i.e., the policy and security requirements set forth by ETSI standards), while in other cases they become mandatory (e.g., in the case of the so-called qualified electronic signature or seal devices, according to CEN standards).

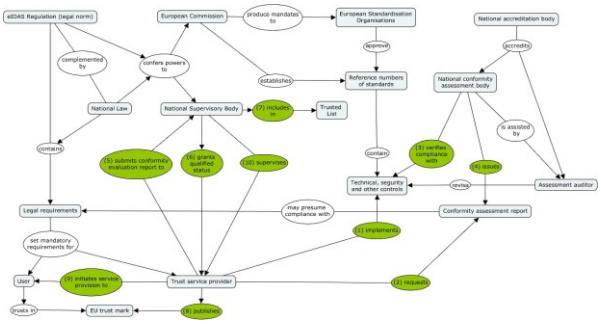

Figure 2. eIDAS Regulatory model conceptual map

It is also interesting to note that qualified trust services have a strict liability regime contained in Article 13 (1) of the eIDAS Regulation. In its virtue, "trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation" (subparagraph 1), and "the intention or negligence of a qualified trust service provider shall be presumed unless that qualified trust service provider proves that the damage referred to in the first subparagraph occurred without the intention or negligence of that qualified trust service provider" (subparagraph 3); while in the case of non-qualified trust services, "the burden of proving intention or negligence of a non-qualified trust service provider shall lie with the natural or legal person claiming the damage referred to in the first subparagraph" (subparagraph 2).

3. *The new legal institution of electronic ledger*

The eIDAS 2 proposal expands the current eIDAS list of trust services with three new qualified trust services, namely the provision of electronic archiving services, electronic ledgers and the management of remote electronic signature and seal creation devices, as a response to the dynamics of the markets and to technological developments.

As stated in the impact assessment section of the proposal, "electronic ledgers provide users with proof and an immutable audit trail for the sequencing of transactions and data records, safeguarding data integrity". Furthermore, "an electronic ledger combines time stamping of data and their sequencing with certainty about the data originator similar to e-signing with the additional benefit of enabling a more decentralized governance that is suitable for multi-party cooperation", pointing clearly to distributed ledger technology.

Some of the potential use cases of this new legal institution include the pooling of data from decentralised sources, self-sovereign identity solutions, attributing ownership to digital assets, recording business processes to audit compliance with sustainability criteria and various use cases in capital markets. Some statistics provided in the proposal try to justify the need for this regulation. In this sense, "75% of all use cases for electronic ledgers were in banking and finance back in 2017. Use cases for electronic ledgers are today increasingly diverse, with 17% in communication & media; 15% in manufacturing & natural resources, 10% in the governmental sector, 8% in insurance, 5% in retail, 6% in transportation, 5% in utilities".

This electronic ledger is characterised, in the same impact assessment section of the proposal, as a "trust service, that builds upon existing trust services as it combines time stamping of data and their sequencing with certainty about the data originator, which is similar to e-signing", which is not really what the proposal says.

Indeed, the detailed explanation of the specific provisions of the proposal clarifies that "the new section 11 establishes a framework for trust services in regards to the creation and maintenance of electronic ledgers and qualified electronic ledgers", following the logic of other eIDAS legal institutions and the associated trust services, as shown in Figure 3, regarding electronic signatures.

[18] I. Alamillo-Domingo, *Identificación, firma y otras pruebas electrónicas. La regulación jurídico-administrativa de la acreditación de las transacciones electrónicas*, Cizur Menor, Aranzadi, 2019, 148; K. Nguyen, *Certification of eIDAS trust services and new global transparency trends*, in *Datenschutz und Datensicherheit*, vol. 7, 2018, 425.

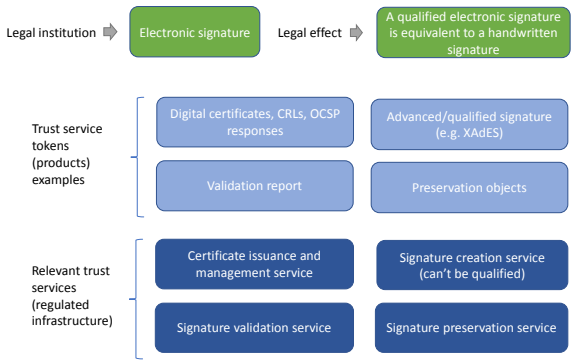

Figure 3. Electronic signature and associated trust services

The application of this eIDAS logic to the electronic ledger is shown in Figure 4.

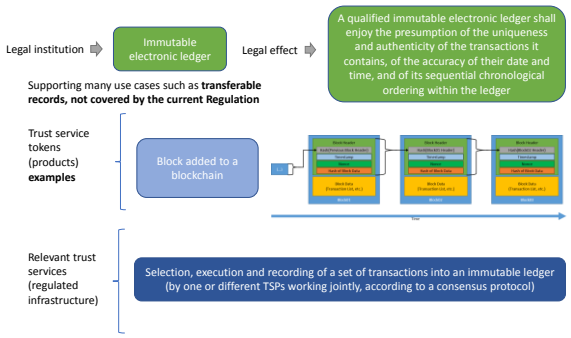

Figure 4. Electronic ledger and associated trust services

In this sense, the proposed regulation is considered "necessary to prevent fragmentation of the internal market, by defining a single pan-European framework that enables the cross-border recognition of trust services supporting the operation of qualified electronic ledgers", following again the usual logic of the eIDAS Regulation.

From a formal legal perspective, Article 1(c) of the eIDAS Regulation is expanded to state that the Regulation "establishes a legal framework for […] electronic ledgers". To this end, a new item 53 of the same Article 3 defines "electronic ledger" as "a tamper proof electronic record of data, providing authenticity and integrity of the data it contains, accuracy of their date and time, and of their chronological ordering".

The legal definition covers both centralised and distributed electronic ledgers, to ensure the technical neutrality of the regulation, in line with other legal institutions and the corresponding supporting or associated trust services.

As with other institutions already supported by the eIDAS Regulation, Article 45h of the eIDAS 2 Proposal defines the legal effects of electronic ledgers.

First, under paragraph 1, "an electronic ledger shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic ledgers", thus applying the non-discrimination principle to electronic ledgers of any sorts.

This is important because it provides a general rule in favour of the legal admissibility of this legal institution, which is currently not granted in all Member States (possibly it is not granted in any Member State, except perhaps Italy, under Article 8-ter of D.L. 14 December 2018, n. 135, confirmed by L. 11 February 2019, n. 12).

Second, and following again the eIDAS logic, under paragraph 2, "a qualified electronic ledger shall enjoy the presumption of the uniqueness and authenticity of the data it contains, of the accuracy of their date and time, and of their sequential chronological ordering within the ledger".

This legal effect partially overlaps with the legal effect of other legal institutions, namely qualified electronic signatures or seals, which ensure the authenticity of data, and qualified electronic timestamps, which ensure the integrity and accuracy of date and time of data.

The novelty is that a qualified ledger ensures two additional properties: uniqueness and sequential chronological ordering of data (within the ledger, or course). As explained in section 1, these two properties cannot be ensured using the other legal institutions alone, which clearly justifies the proposal.

4. *A trust service for electronic ledgers*

A new item (f) of Article 3(16) of the eIDAS Regulation define a new specific trust service, which consists in "the recording of electronic data into an electronic ledger". Recall that a trust service is an electronic service normally provided for remuneration, which is offered by a so-called trust service provider, which is a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider, as introduced before.

Therefore, it is of paramount importance to identify who exactly is the trust service provider,

something that will vary depending on the type of electronic ledger being created.

First, permissionless distributed electronic ledgers may not benefit from the eIDAS Regulation, because they operate under pseudonyms and do not submit to any supervisory regime.

Second, while in a centralised ledger approach it is easy to determine who provides the service, it may be difficult to do so when it comes to decentralised ledgers, where there are several roles involved, including the so-called miners, minters, validators or orderers, and regular nodes, depending on the consensus protocol. Are all these roles to be considered as trust service providers? Attending to the trust service definition, only distributed ledger actors recording electronic data into the ledger are to be subject to the regulation (of course, when they offer their service to the public, as happens with any trust service).

Article 45i(1) of the eIDAS 2 Proposal contain the legal requirements for creating qualified electronic ledgers, including the need to be created by one or more qualified trust service provider or providers –allowing centralised and distributed ledgers–; to ensure the uniqueness, authenticity and correct sequencing of data entries recorded in the ledger; the correct sequential chronological ordering of data in the ledger and the accuracy of the date and time of the data entry; and to record data in such a way that any subsequent change to the data is immediately detectable.

Article 45i(1) refers to the creation of the qualified electronic ledger, this signalling that the recording of information into the ledger is done by any actor who actually creates this ledger; therefore, in a distributed ledger environment such as a blockchain, the trust service provider will be, normally, any actor intervening in the creation of blocks. For instance, in the case of Proof of Authority under IBFT 2.0[19] used in the EBSI, these will be the validator nodes, including those proposing blocks and those confirming blocks (using their electronic seals, by the way), but not the regular nodes.

How these requirements are fulfilled will heavily depend on the functioning of the electronic ledger technology, of course. Thus, the role of the standardization activities is of paramount importance. This is recognised in Article 45i(2), which states that "compliance with the requirements laid down in paragraph 1 shall be presumed where an electronic ledger meets the standards referred to in paragraph 3".

Such standards may be established by the European Commission, by means of implementing acts adopted in accordance with the examination procedure referred to in Article 48(2), and they will be referred to the processes of execution and registration of a set of data into, and the creation, of a qualified electronic ledger. Interestingly, this is the only paragraph where the proposal refers to the execution over data capability of the ledger, in a clear reference to the so-called smart contracts.

Of course, there may be other legal requirements applicable to the trust service provider(s) offering the service, as stated in Whereas (35), "this trust service for electronic ledgers and qualified electronic ledgers and the certification as qualified trust service provider for electronic ledgers should be notwithstanding the need for use cases to comply with Union law or national law in compliance with Union law", citing GDPR but with a clear focus in use cases that involve crypto assets, which "should be compatible with all applicable financial rules for example with the Markets in Financial Instruments Directive, the Payment Services Directive and the future Markets in Crypto Assets Regulation".

5. *Conclusions*

The eIDAS 2 Regulation can be seen as a baseline, general regulation for all electronic ledgers and the associated trust service, defining a generic legal effect and recognition in cross-border transactions, facilitating it adoption in the Digital Single Market, and legal certainty to all use cases relying in electronic ledgers.

It represents a bold, novel, approach to the regulation of distributed ledgers technologies, but it implies important challenges in order to its sound application, especially from the perspective of the adoption of technical regulatory standards.

[19] R. Saltini and D. Hyland-Wood, *IBFT 2.0: A Safe and Live Variation of the IBFT Blockchain Consensus Protocol for Eventually Synchronous Networks*, presentend at IBFT 2.0, Istanbul, 2019.